30 OCT 1984

MEMORANDUM FOR THE RECORD

25X1

FROM: [redacted]
Industrial Security Branch

SUBJECT: Highlights of Speakers' Remarks at the Industrial Security Seminar of 15 - 17 October 1984

I. Opening remarks by the Office of Security [redacted] Deputy Director of Security [redacted], Chief of the Physical Security Division; and [redacted] Chief of the Industrial Security Branch. 25X1 25X1 25X1

° Stressed the overall success of industry in meeting the needs of security and the need for continued teamwork.

° Discussed the fact that one-third of the resources of the Agency's Office of Security is committed to industry.

° Stressed the need to build a security awareness program and the need for company security officers to "get to know" the people they are submitting for clearances.

° Outlined the general differences between covert and overt contractual agreements and the fact that the Agency's Contract Technical Representative (COTR) is the company's first line of contact with Agency personnel.

° Discussed the fact that after audit recommendations are made the contractor has 45 days to respond to same. Also, outlined the basic way this is accomplished.

° Made aware that, in addition to the audit by the Industrial Security Branch, there are other kinds of checks and balances, i.e., the computer security audit, polygraph tests, the audits by the Office of Communications' staff and the Office of Finance.

WARNING NOTICE
Intelligence Sources
or Methods Involved

[redacted] 25X1

II. Remarks by Charles Briggs, Director of Legislative Liaison, CIA.

° There has been increased emphasis on security following the Boyce-Lee case occurring six years ago. 25X1 Examples are that [redacted] audits of contractors have been conducted and the Agency has doubled the number of security officers assigned to contractors.

° Computer security has now become a major concern in that there is concern about the problem of controlling access to the building where the computers are stored. Other computer security concerns involve controlling the keys to areas, codes to the terminals and securing the hardware and software of programs.

° There are increased security concerns in the entire intelligence community as time goes on and as technology advances are made: the community can now receive real time information, technical data is now linked to computer systems (physical distances between these systems must be secured). In addition, increased numbers of NATO officials have access to Agency material.

° The press has given the public the impression that CIA has an adversarial relationship with Congress although, in reality, this is not true. What has been publicized is the categorical disagreement between the two groups on the manner in which Latin American policy should be run and, as such, the Agency has become the "whipping boy" of members of the press.

° In the FY 1985 budget there were only cuts in Agency programs in Latin America. Other programs seem to have benefitted through increases in the intelligence capability. In the past three of four fiscal years, the Agency began construction of the new building, major modifications of NPIC have been made and the FBIS has been modernized.

° Another major victory for the Agency this fiscal year is with regard to the Freedom of Information Act in that the Agency is no longer required to search its operational files of the Directorates. In the past, the Agency could delete those operational files dealing with sources and methods but the process to sort this out was difficult. Legislation involving the Freedom of Information Act always affects the Agency's relationship with covert targets and with foreign liaison services--the relationship is good when files are restricted and adversarial when file information has the potential for being widely disseminated.

° The Agency continues to recieve many job applicants yearly and currently, from the 200,000 received, only 1200 people are hired.

° Security concerns in the area of leaks to the news media were also discussed and the inherent problem that as more and more people have access to classified information, there is more potential for unauthorized disclosures.

III. Remarks by Chief, Security Staff, Office of Development and Engineering (OD&E) of the Directorate of Science and
25X1 Technology - [redacted]

° Discussed the contractor award fees and fact that industry receives same for good technical management as well as good security.

° Presented viewgraph on structure of the Security Staff of OD&E and specifically mentioned that there is now one individual assigned to computer security
25X1 there [redacted]

° Discussed fact that there are 21 couriers who consistently work more overtime than any airline crew. Because of this, stressed the reasons for the contractor to evaluate need for their services in order to avoid misuse.

° Discussed the procedures for processing industrial approvals: (1) contractor identifies the candidate; (2) the contractor security staff reviews the candidate; (3) the request is submitted to OD&E; (4) the COTR verifies that a particular clearance or approval is needed; (5) OD&E Security Staff notifies contractor to proceed with request; (6) the paperwork is submitted to the OD&E Security Staff; (7) the paperwork is submitted to the Agency's Clearance Division where a file is set up and the background investigation is assigned [redacted]. 25X1

° Sometimes the reason for the delay in granting a security approval is that the individual has not filled out the paperwork in the proper manner.

° The other reason for the delay is that the company security officers are not forwarding requests promptly. In some cases it has taken three weeks for cases to be forwarded.

° The current processing time for industrial approvals is between 160 and 170 days.

° Discussed revisions to the BYE Industrial Security Manual (BISM): (1) on the issue of employees' foreign travel, the contractor is to now report only significant cases and the information involving travel to Soviet Bloc countries. The contractor will be required to maintain a log of all foreign travel undertaken by program approved employees; (2) the safe combinations are to be changed every year in lieu of the current standard that requires change every six months; (3) the contractor is to notify Headquarters on any employees' forthcoming legal proceedings; (4) the contractor is encouraged to request a BYE administrative (BYA) approval in lieu of the current need to request total BYE approval on employees. BYA approval requests should be used for contract/admin support personnel including clerks, couriers, health and safety specialists, etc. (5) the contractor is encouraged to request Proximity (PROX) approvals for employees who have no need to be briefed on the entire program. An example is that a guard may be given a Proximity approval since there is only a possibility that he/she might see a sensitive part of the program. Employees who receive Proximity approvals sign secrecy agreements which are not SCI binding; (6) Agency security staffs will add the computer security requirements to the BISM.

A Rose By Any Other Name...

° Discussed problems inherent to restricting the access of an employee who formerly held all accesses. There could be a morale problem, i.e., "the employee's feeling that he/she is not trusted anymore."

° Discussed the goals of the Directorate of Science and Technology:

(1) strive for excellence;
(2) adopt an effective security education program involving discussion of media contacts and reporting same, leaks, publications, foreign national contact, foreign travel and an employee's changes in his/her permanent status (changes of marital status, etc.);

(3) on clearance requests, individual should be a person who definitely needs a clearance and the request should be submitted with a justification. There should also be adequate briefing and debriefing programs involving a thorough understanding of the secrecy agreement and phases of security accesses;

(4) the OD&E Security Staff will continue to establish physical security requirements for the SCIFs; ?

(5) the OD&E Security Staff will continue to stress compliance with requirements of the BISM on document control, courier procedures, registry procedures, etc.

IV. Remarks by Industrial Security Branch Officer [redacted] 25X1

° Outlined the character of the Branch and presented viewgraphs on the structure of the office.

25X1 V. Discussion by [redacted] Chief of the Clearance Division, on the Industrial Security Approval Process.

° Discussed the allocation of resources in the Clearance Division.

° Presented the fact that approvals/clearances that are granted sometimes involve a matter of judgement. Most cases are not clear-cut.

° In FY 1984, 10,000 files were handled for granting people additional accesses.

° There were 28,000 form 2018As handled.

° At the current time there are 3,000 pending cases.

° A relatively small number of cases are disapproved.

° 170 days is currently the average processing time for approvals.

° Discussed the risk factor in granting employees approval and the vulnerabilities an individual may have (financial, loyalty, drug use, emotional stability, etc.).

° The number one reason for security disapprovals is a person's illegal drug use. The second biggest reason is some type of criminal activity, mainly thefts.

25X1 VI. Remarks by [redacted] Office of General Counsel, on the legal aspects of the Industrial Security approvals and appeals.

° There should be mutual expectations by both the contractor and Agency in that some pre-screening should be done and the people who obviously do not meet standards should be kept out.

° Suggested that the contractor's legal staff might include in their contracts the standards for specialized accesses. In this way the contractor could require that damages be paid in the case of a denial for the time it took for an employee to be cleared.

° Generally discussed why investigative procedures are employed and stressed the need for the "whole person concept" in evaluating an individual's risk potential.

° Stressed that the procedures for granting approvals involve risk assessment and management.

° Any doubt on whether a person should be granted access to classified material is resolved in favor of national security.

° Discussed the appeals process and generally discussed the function of the Industrial Review Panel.

° One of the jobs of the Office of General Counsel is to defend the judgements of the Office of Security but, in order to do that, the defense must be discussed early and the defense must make sense.

° The Department of Defense routinely litigates in cases where appeals are made. The CIA does not because the CIA does not believe that there is a constitutional basis for an individual's case against the U.S. Government.

° In granting people security approvals, the CIA's intent is not to standardize behavior.

VII. Discussion on the Industrial Polygraph Program by 25X1 [redacted] of the Polygraph Division.

° Since the industrial polygraph was initiated, 25X1 [redacted] contractors have participated in the program and approximately 6,000 have been completed. In addition, 25X1 there have been over [redacted] polygraph charts run.

° Stressed the need for properly briefed individuals on the polygraph program.

° One of 20 cases where the polygraph is used require adjudication.

° When the polygraph examiner receives information indicating a violation of federal law, that information is provided to other government agencies. In addition, derogatory information affecting national security will also be reported in this manner.

VIII. Workshop Forum - all seminar attendees participated.

° Discussed the revisions to the BISM and concerns about same were exchanged:

(1) Use of the BYA and Proximity should be further clarified and not appear so nebulous.
(2) Unless some provisions are made, there would be no way to tell from an employee's badge what accesses he or she possess.
(3) Who decides who gets what briefing and what information is provided in the briefing?
(4) What would these individuals be told in their debriefing?
25X1 (5) Are programs [redacted] being involved in this procedure?

IX. Remarks on document control by [redacted] of the Special Security Center. 25X1

° Discussed difference between collateral and SCI material.

° Discussed levels of information: Categories I, II and III and the codewords of each.

° Discussed the manner in which the working papers should be handled and fact that the document should either be held in accountability or destroyed after 90 days.

° Documents are controlled with a number preceded by an SC (indicating special channel information).

° The number appearing after the slash (/) means that the document is draft 1, draft 2, etc. (Example:
25X1 [redacted]

° When the product is finalized, the drafts are destroyed and the control number becomes the original number.

° Discussed the classifications WINTEL, ORCON, No Contract, PROPIN, NOFORN, REL TO.

X. Approved Destruction Equipment and Destruction Guidelines
25X1 by [redacted]

° Discussed methods of destroying microfiche and magnetic tape and pros and cons of using each method.

° Discussed standards for use of filter screens in the destruction devices.

° The cross-cut shredder is the only shredder approved by CIA; other agencies approve the strip shredder.

25X1 XI. Telephone Systems - [redacted]

° Discussed security problems inherent to the use of the new computer-based main switch which has replaced the old electrical mechanical switch. With the computer-based switch, [redacted] the software so they essentially control the switch. 25X1

° Associated auxiliary equipment is a security threat especially when used for remote maintenance and testing.

° There are now commmunity-wide guidelines established for using the dimensional switches. For example, with a dimensional switch, a touch-tone is not needed but a dial phone may be used.

° A foreign-owned or controlled company is not to be involved in the installation of SCIF telephone systems.

XII. Information systems security overview by [redacted] 25X1

° Discussed the charter of the Information Systems Security Group (ISSG):

(1) they interpret the rules for the contractors;
(2) they review the contractor's ADP security plan for approval prior to installation;
(3) they sometimes act as brokers with COMSEC (Office of Communications Security Group).

° Discussed the several modes for security data-processing systems:

(1) Dedicated mode used for one program for one NFIB member (National Foreign Intelligence Board) for either full-time or for a specified period of time.
(2) System high NFIB for two or more programs and one NFIB member. In this case all users must have valid security accesses for all contracts.
(3) System high mode for two or more NFIB members and two or more programs. All users must have full access approvals and the cognizant security officer is to be identified.

(4) Multi-compartmented for two or more SCI programs and two or more NFIB members. Users are not cross-cleared. There are now four multi-compartmented systems in use. The VAX system cannot support multi-compartmented modes of operation.

° Another security concern involves classified terminals inside the SCIF which are connected to unclassified computer systems.

° All terminals in SCIFs are to be hard wired to corporate computer systems. Dial-up modems are not to be used.

° Classified systems are to be physically located away from unclassified systems in the SCIFs and clearly marked as such.

° Once a personal computer is used in a SCIF it is not to be removed.

? WHY ?
SEE cover SHEET

° For use of Winchester discs, contractor needs waiver for open storage (when the power of the unit is turned off, all the information stays on the disc).

° Sanitization of tapes and magnetic media is a security problem in that some are impossible to degause and whether a medium can be overwritten is still a controversial topic.

° Decisions on whether to allow overwrites is to rest with the program managers.

° Password management is a security problem and, at present, passwords are controlled by the system's administrator.

° Magnetic media must be controlled and classified in the same manner as hard copy.

° Contractors must submit the full configuration chart for ISSG to analyze the complete system.

XIII. Technology loss affecting national security by [redacted] 25X1

25X1 [redacted]

25X1

[redacted]

XIV. Workshop Forum - all seminar attendees participated

° The audit process and the history and philosophy of the audit staff were discussed.

° Auditors have been able to emphasize to company management those security concerns which the company security officer has had difficulty receiving support on in the past.

° The feeling of those contractors who have already been audited is that the auditors provide a "fresh look."

° Ninety percent of the problems the auditors find are in the document control area.

XV. Security Awareness Programming for Industry [redacted] 25X1

° Must identify objectives of program:

(1) keep people thinking about security;
(2) raise literacy level and make people understand security concerns.

° Use active methods for security education (briefings) and passive methods (posters, handouts, etc.)

° Use examples and discuss espionage cases if necessary, i.e., Moore case, Kampiles case.

° Must realize that approach must be that of a salesman and the program should be voluntary, although there should be some mandatory sessions.

° May use information available through any associations which the company security officer may be involved. An example is the American Society for Industrial Security.

° May receive much information from newspapers.

° Other sources are John Baron's book, The KGB Today.

° May use video recorders to tape news presentations and then later excerpt and present as part of program.

° Use DoD security awareness bulletins.

° May break down the security awareness in several parts and outlined the program provided to new CIA employees:

I. History of Intelligence
   a. CIA and the intelligence community
   b. Security in intelligence
   c. Hostile intelligence threat
   d. Espionage cases

II. Hostile Audio Surveillance
   a. Telephone security
   b. Physical security
   c. Outside activities
   d. Function of the Security Duty Office

III. Safety Program/Security Violations
   a. Security in public areas
   b. Personnel security
   c. Execution of secrecy agreement

° May also ask to participate in the program provided through the FBI.

° May use first person stories, i.e., an individual who has been approached by an intelligence service may tell how that occurred.

° May use various "white papers" of the community, i.e., "The Spies Among Us," by the Department of Defense.

XVI. Leaks of classified information b[redacted] 25X1

° Showed tape made by the DCI on this issue.

° Human assets who provide information later leaked to the press tend to refuse to cooperate with the U.S. in the future.

° Gave several examples of leaks and provided specific information on the damage caused by the leaks.

° Cited the leaks on the SS-20 missiles, pointing out that Evans and Novak received their information from several sources and pieced together bits and pieces to arrive at the final story.

° Addressed specific steps to prevent disclosure and strongly suggested that the National Intelligence Daily (NID) should be placed under stricter controls.

° Gave two examples of recent cases of unauthorized disclosures. In one case, a senior Agency official was fired and, in the other, the individual received a warning.

° CIA employees are constantly made aware of responsibilities in dealing with the press. Should not say "no comment" since this is currently viewed as a confirmation of the story. Should instead say "we do not discuss certain matters."

° Discussed the potential leak damage:

(1) loss or arrest of agent;
(2) loss of cooperation with a foreign government;
(3) capabilities may be compromised;
(4) subject U.S. to risk of collecting disinformation.

° There were 936 leaks from FY 1972 to FY 1984; 486 were duplicate leaks and 85 came from Jack Anderson.

° There is a new perception of leaks: they are harmful to national security; they are helpful to foreign governments; they are reprehensible breaches of trust and they are costly to U.S. taxpayers.

XVII. Closing remarks by [redacted] 25X1

° Hoped that the goal of the seminar was the opening of communications and continuance of opened communications between the contractor and CIA.

° Discussed future goals for the Office of Security, i.e., more timely security approvals. The average processing time for staff applicants is now 75 days. On the other hand, the average processing time for industrial security security approvals is now is 175 days. Intend to make 120 days the goal in the future.

° The company security officer should view responsibility in several areas:

(1) Personnel security - do not nominate for approvals those people who are not "worthy"; do not nominate beyond the needs of the program; do not look to CIA to solve company's management problems; keep accurate records;

(2) Physical security - follow the standards that have been provided for them;

(3) Computer security - efforts to concentrate on establishing manner for performing audit trail; develop system to guarantee compartmentation of audit.

(4) Effective security awareness programs.

CONFIDENTIAL

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Highlights of Speakers' Remarks at the Industrial Security Seminar of 15-17 October 1984

25X1 FROM: [redacted]
Industrial Security Branch
25X1 [redacted]

EXTENSION: [redacted] 25X1

NO.

DATE: 30 October 1984

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS
1. AC/ISB		10/31/84	TB
2.			
3. DC/PSD		11/4/84	JR
4.			
5. C/PSD	NOV 1984	5 Nov	B
6.			
7. C/OPS/PTAS	5 NOV	11/5	C
8.			
9. DD/PTAS		11/9	RV
10. C/PSD — info			B
11. C/ISB Action		11/14/84	JAA
12. [redacted]		11/19/84	CK
13.			
14.			
15.			

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

This is in response to a specific request made by DD/PTAS for highlights of the speakers' remarks at the Industrial Security Seminar.

11 to 12

Good JOB, CAROL

[redacted] 25X1

Jim:

— Please thank Carol & continue to follow the big meeting & industry reaction over [illegible]

[redacted] 25X1

Chief, [illegible]

CONFIDENTIAL